



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/893,408	06/29/2001	Daniel Buttiker	109988	6019
25944	7590	10/18/2004	EXAMINER	
OLIFF & BERRIDGE, PLC P.O. BOX 19928 ALEXANDRIA, VA 22320			SHIFERAW, ELENI A	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 10/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/893,408	Applicant(s) BUTTIKER, DANIEL	
	Examiner Eleni A Shiferaw	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>10/01/2001</u> . | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-20 are presented for examination.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al (Hind, Pub. No.: US 2003/0212893 A1) in view of Matyas, Jr. et al. (Matyas, Patent No.: US 6,687,375 B1).

3.1 As per claim 1, Hind teaches method for registering users of a public-key infrastructure based on credentials of a user, including biometric data such as data related to a fingerprint, presented to an authority (100) of the public-key infrastructure, comprising the steps of

a) connecting a token (10), which comprises a processor (2), an interface device (3) and a memory device (5), containing a private-key (51) and a public-key (52) for the user of the token (10) and a private-key (53) issued by the authority (100); to a terminal (20, 30) capable to access the network (200) of the public-key infrastructure (Hind Fig. 6 No. 510, connecting smart card),

b1) reading biometric data (58) of the user, such as data derived from a finger print of the user, by a biometric input device (1; 31) (Hind Page 8 par. [0076-0077]);

b2) signing the biometric data (58) with a key of an asymmetric or symmetric key pair or by means of a shared password issued by the authority (100) (Hind Page 3 par. 0029, page 7 par. 0060);

b3) sending a certification request, containing the public-key (52), signed biometric data (58) and additional credentials of the user, to the authority (100) (Hind Page 8 par. 0068);

c1) verifying and registering the received data by the authority (100) (Hind Page 3 par. 0031-0032); and

c3) returning a corresponding certificate (520) (Hind Page 8 par. 0068);

Hind does not explicitly teach c2) storing the biometric data (58) in a database (104);

d) storing the certificate (520) in the token;

However Matyas teaches c2) storing the biometric data (58) in a database (104) (Matyas Col. 14 lines 48-61);

d) storing the certificate (520) in the token (Matyas Col. 8 lines 42-53);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Matyas with in the system of Hind because it would potentially allow an easy mechanism for the user to prove their identity, especially if the

user carries their biometric certificate on a portable token (e.g. smart card) (Matyas Col. 8 lines 41-53); and biometric templates are stored in a central data base and the given biometric data are compared with the set of biometric templates stored in a central data base to authenticate user identity.

3.2 As per claim 12, Hind teaches token (10) designed for registering users at an authority (100) of a public-key infrastructure particularly according to the method of claim 1, comprising a processor (2), a memory device (5), an operating system (4) and an interface device (3) designed for exchanging data with a terminal (20, 30) which is capable to access the network (200) of the public-key infrastructure, characterized in that

a) the memory device (5) contains a private-key (51) and a public-key (52) for a user of the token (10) and a private-key (53) issued by the authority (100) (Hind Page 10 par. 0089, Fig. 6 No. 510, & 150);

b) the token (10) is capable of processing biometric data (58) read and transferred from an internal or external biometric input device (31) (Hind Page 9 par. 0077);

c) the token (10) is capable of signing the read biometric data (58) with a key of an asymmetric or symmetric key pair or by means of a shared password issued by the authority 100) (Hind Page 3 par. 0029, page 7 par. 0060);

Hind does not explicitly teach d) the token (10) is capable of storing a certificate (520) which has been issued by the authority (100) based upon a certification request originating from the token (10).

However Matyas teaches d) the token (10) is capable of storing a certificate (520) which has been issued by the authority (100) based upon a certification request originating from the token (10) (Hind Page 8 lines 42-53)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Matyas with in the system of Hind because it would potentially allow an easy mechanism for the user to prove their identity, especially if the user carries their biometric certificate on a portable token (e.g. smart card) (Matyas Col. 8 lines 41-53).

3.3 As per claim 2, Hind teaches method comprising the steps of double signing the biometric data with said key of an asymmetric or symmetric key pair or by means of a shared password and the user's private key (51) (Hind Page 8 par. 0068).

3.4 As per claim 3, Hind teaches method, with a serial number of the token being stored in the memory device (5), which, included in the certification request, is sent to the authority (100) which, based on said serial number, retrieves the symmetric or asymmetric key or the password matching the key or password used for signing the biometric data (58) in order to decrypt the signed message (Hind Page 6 par. 0059).

3.5 As per claim 4, Hind teaches method, for a public-key infrastructure with an authority

(100), consisting of a registration authority (101), a certification authority (102) and a key and certificate management unit (103), comprising the steps of issuing for each token (10) an individual symmetric or asymmetric key-pair, a first key stored in the token (10) for signing the biometric data (58) and a second key (54) stored at the registration authority (101) (Hind Page 8 par. 0068).

3.6 As per claim 5, Hind teaches method, with the public-key (54; 55) of the registration authority (101) and or the certification authority (102) being stored in the token (10), comprising the steps of encrypting at least the part of the certification request containing the biometric data with one of said public-keys (54; 55) before sending it and decrypting the received certification request by the registration authority (101) with the corresponding private-key (53, . . .) (Hind Page 7 par. 0060, page 12 par. 0102).

3.7 As per claim 6, Hind teaches method, with the biometric input device (31) being integrated in the token (10) comprising the steps of pressing a finger onto the token (10) while biometric data (59) is read (Hind Page 6 pr. 0056).

3.8 As per claim 7, Hind teaches method, comprising the steps of storing the biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5) (Hind Page 8 par. [0075-0076]).

3.9 As per claim 8, Hind teaches method, comprising the steps of comparing a password

entered with the password stored in the token (10) and/or reading biometric data from the user and comparing biometric data read with biometric data (58) stored in the token (10) or in the database (104) of the authority (100) and providing access to the system in case that the compared data match and/or storing mismatched data as proof for legal prosecution of a non-authorized user of the token 10 (Hind Page 8 par. 0075).

3.10 As per claim 9, Hind teaches method, comprising the steps of generating the key pair for the user, the private-key (51) and the public-key (52) within the token (10) (Hind Page 7 par. 0060).

3.11 As per claim 10, Hind teaches method, comprising the steps of performing transactions defined by the authority of the public-key infrastructure while using the registered token (10) (Hind Page 5 par. 0051).

3.12 As per claim 11, Hind teaches method, comprising the steps of keeping the user's data, particularly the biometric data, private except for cases of fraud (Hind Page 8 par. 0076).

3.13 As per claim 13, Hind teaches token (10) capable of signing the read biometric data (58) with the key of the asymmetric or symmetric key pair or by means of a shared password and the user's private key (51) (Hind Page 8 par. 0068).

3.14 As per claim 14, Hind teaches token (10), with a serial number of the token being stored

in the memory device (5) (Hind Page 6 par. 0059).

3.15 As per claim 15, Hind teaches token (10), for a public-key infrastructure with an authority (100), consisting of a registration authority (101), a certification authority (102) and a key and certificate management unit (103), comprising an individual key of a symmetric or asymmetric key-pair or a shared password for signing the biometric data (58) and a public-key (55) issued by the registration authority (101) or the certification authority (102) for encrypting the certification request sent to the authority (100) (Hind Page 8 par. 0068, page 7 par. 0060).

3.16 As per claim 16, Hind teaches token (10), with the biometric input device (1) being integrated in the token (10) (Hind Page 8 par. 0076).

3.17 As per claim 17, Hind teaches token (10), designed to store the read biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5) (Hind Page 8 par. 0076).

3.18 As per claim 18, Hind teaches token (10), capable to compare a password entered with the password stored in the token (10) and/or capable of reading biometric data from the user and comparing biometric data read with biometric data (58) stored in the token (10) providing access to the system in case that the compared data match (Hind Page 8 par. 0069, 0075, & 0076).

3.19 As per claim 19, Hind teaches token (10), capable to generating the key pair for the user,

the private-key (51) and the public-key (52), within the token (10) (Hind Page 7 par. 0060).

3.20 As per claim 20, Hind teaches registration system (35) providing access to a token (10) according to claim 12 with a terminal (30) designed to exchange data with the network (200) of the public-key infrastructure, with a connected token (10) and with at least one biometric input device (31) capable of reading biometric data, preferably as data related to a fingerprint, the retina, the face and/or the voice of a user which biometric data is transferable via the terminal (30) to the token (10) for processing (Hind Page 5 par. 0051, page 6 par. 0056, page 7 par. 0065, and page 8 par. 0076).

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 09/893,408
Art Unit: 2136

Page 10

Eleni Shiferaw
Art Unit 2136


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100